A shift column different offset for better Rijndael security

ABSTRACT

The strength of an encryption algorithms depends on the keyôs secrecy combined with the structure of the block cipher that is able to produce random output. The goal of a strong symmetric key encryption algorithm is that there is no way to decrypt the data except by knowledge of the key and there is no better way to find out that key than key exhaustion [1]. The secrecy of an encryption algorithm is measured in terms of the computational power and time required to extract the secret key. The security of the algorithm on the other hand, is based on the randomness of the output from the encryption process. This is the result of a combination of strong key and the structure of the block cipher. Rijndael, currently the Advanced Encryption Standard Algorithms (AES) is a block cipher uses a 128, 192, or 256-bit key length to encrypt 128-bit blocks of plaintext. Structurally, it has larger S-boxes, but a very simple algebraic description that make it particularly vulnerable [3]. This paper proposes a transformation function to be added to the Rijndael algorithm. It is called a ColumnShift() with different offset values that is added to the currently four transformation functions. The main objective is to increase the security of the encryption. A comparison between the Rijndael algorithm and the new approach shows that the security or the randomness by the proposed approach is better than the Rijndael.

Keyword: AES; Rijndael; Transformation function; Randomness; Security; Cryptography